AMENDMENTS TO THE CLAIMS

The listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Currently Amended) A system for enhancing security of end user station access to an Internet and intranet~~(s), e.g. of corporate access,~~ over access network with an access ~~points~~ point, comprising:

a gateway packet data node; ~~nodes (3A, 3B),~~

a packet data support node; ~~nodes (2 ; 2,2'), characterized in~~

~~that it~~ wherein said gateway packet data node further comprises security indication providing means ~~(11 ; 12; 13;11A, 11B ; 12A, 12B; 13A, 13B)~~ for providing an ~~(corporate)~~ security indicated access point with a security criterium indication ~~(defining security)~~ and for distributing said security criterium indication to ~~a~~ said packet data support node; ~~(2 ; 2,2'), and in that~~

wherein said packet data support node further comprises a security enforcement mechanism ~~(21;211,21A ; 21B) is provided in the packet data support node (2 ; 2,2'), said security enforcement mechanism at least providing~~ for preventing all other traffic not fulfilling the security criterium indication ~~conflicting the~~ associated with said security indicated access point when there is a connection requiring security over the security indicated access point, at least until the last packet of the security indicated access point connection has been sent.

2. (Currently Amended) A system according to claim 1, ~~characterized in~~ wherein that the security criterium indication comprises a security marking indicating that the access point supports the provision of secure access point connections.

3. (Currently Amended) A system according to claim 1, ~~characterized in that~~ wherein the security criterium indication comprises an indication as to the criterium~~/criteria~~ that ~~is/are~~ is to be fulfilled for concurrent conflicting access point

connections in order for them to be allowed simultaneously with a first secure access point connection.

4. (Currently Amended) A system according to claim 2 ~~or 3~~, ~~characterized in~~ wherein that the security criterium/~~criteria~~ indication comprises a flag, an attribute or a data structure.

5. (Cancelled)

6. (Currently Amended) A system according to ~~any one of the preceding claims~~ claim 1, ~~characterized in~~ wherein that the gateway packet data node comprises a Gateway GPRS Support Node (GGSN).

7. (Currently Amended) A system according to ~~any one of claims 1-4~~ , ~~characterized in~~ claim 1 wherein that the security indicating and distributing means are provided in a Home Location Register (HLR).

8. (Currently Amended) A system according to ~~any one of claims 1-4 and 6~~ claim 1, ~~characterized in~~ wherein that the security indicating and distributing means are provided in a Domain Name Server (DNS).

9. (Currently Amended) A system according to ~~any one of the preceding claims~~ claim 1, ~~characterized in~~ wherein that the security indicating means are provided in a CGSN comprising the functionality of a GGSN and SGSN.

10. (Currently Amended) A system according to ~~any one of the preceding claims~~ claim 1, ~~characterized in~~ wherein that an access point is security indicated through providing an Access Point Name ~~(APN)~~ thereof with the security indication, e.g. an attribute.

11. (Currently Amended) A system according to ~~any of the preceding claims~~ claim 1, ~~characterized in~~ wherein that access point connections comprise Packet Data Protocol (PDP) ~~PDP~~ contexts.

12. (Currently Amended) A system according to claim 11, ~~characterized in that~~ wherein the enforcement mechanism is dynamic, and in that in the packet data support node ~~(SGSN; CGSN)~~ means are provided for dropping all ~~traffical~~ traffic packets of other PDP contexts not meeting the security ~~criterium/criteria~~ criterium when a simultaneous PDP context to a security marked access point is used for communication of packets.

13. (Currently Amended) A system according to claim 12, ~~characterized in~~ wherein that the packet data node ~~(SGSN, CGSN)~~ comprises means for detecting traffic on a PDP context to a security indicated access point, and means for activating security protection and in that it further comprises means for, after lapse of a predetermined, configurable time period after sending of the last packet on a PDP context with a security indication, allowing traffic on other PDP contexts again.

14. (Currently Amended) A system according to ~~any one of claims 1-11~~ claim 1, ~~characterized in~~ wherein that the enforcement mechanism is static and in that means are provided in a packet data support node~~, e.g. SGSN or CGSN,~~ for deactivating access point connections~~, e.g. PDP contexts,~~ which do not meet the security ~~criterium/criteria~~ criterium when a security condition is met for one connection to a security indicated access point.

15. (Currently Amended) A system according to claim 14, ~~characterized in~~ wherein that a security condition is met when a request is received in the packet data support node ~~(SGSN; CGSN)~~ relating to activation of a PDP context to a security indicated APN.

16. (Currently Amended) A system according to claim 14, ~~characterized in~~ wherein that a security condition is met when a PDP context to a security marked APN has been activated in the packet data support node.

17. (Currently Amended) A system according to claim 14, ~~characterized in~~ wherein that a security condition is met when traffic packet is detected on a PDP context to a security indicated access point.

18. (Currently Amended) A system according to claim 16 ~~or 17~~, ~~characterized in~~ wherein that the packet data support node comprises means for re-activation of deactivated PDP contexts, and in that said means ~~e.g.~~ are end user controlled.

19. (Currently Amended) A packet data support node ~~(PDN; SGSN; CGSN) (2 ; 2,2')~~ for enhancing security at end user station access to Internet and ~~intranet(s), e.g. corporate access, characterized in that it comprises~~ intranet, said packet data support node communicating with a gateway packet data node including security indication providing and distributing means, comprising:

a security enforcement mechanism~~, said security enforcement mechanism~~ comprising means for receiving and detecting an access point security indication from a said security indication providing and distributing means within said gateway packet data node,

traffic preventing means for preventing all other traffic not fulfilling ~~(a) security criterium/criteria~~ a security criterium conflicting with a security indicated access point connection at least until the last packet of the security indicated access point connection has been sent.

20. (Currently Amended) A packet data support node according to claim 19, ~~characterized in~~ wherein that security indication comprises a number of criteria to be fulfilled by ~~concurrent/conflicting~~ concurrent access point connections in order for them to be allowed simultaneously with other secure access point connections.

21. (Currently Amended) A packet data support node according to claim 19 ~~or 20, characterized in~~ wherein that the security indication comprises an Access Point Name (APN) indication.

22. (Currently Amended) A packet data support node according to claim 21, ~~characterized in~~ that it comprises an SGSN.

23. (Currently Amended) A packet data support node according to claim 21, ~~characterized in~~ wherein that it comprises a CGSN.

24. (Currently Amended) A packet data support node according to claim 22 ~~or 23, characterized in~~ wherein that the access point connections comprise PDP contexts.

25. (Currently Amended) A packet data support node according to claim 24, ~~characterized in~~ wherein that the enforcement mechanism is dynamic, providing for dropping of all traffical packets of all PDP contexts not meeting the security criterium~~/criteria~~, but keeping the PDP contexts.

26. (Currently Amended) A packet data support node according to claim 25, ~~characterized in~~ wherein that it comprises

means for detecting traffic on a PDP context to a security indicated access point ~~(APN)~~, and

means for activating security protection and in that it further comprises

means for, after lapse of a predetermined, configurable time period after sending of the last packet on a PDP context to a security indicated access point, allowing traffic on other PDP contexts.

27. (Currently Amended) A packet data support node according to claim 24, ~~characterized in~~ wherein that the enforcement mechanism is static and in that the packet data support node comprises means for deactivating access point connections, ~~e.g. PDP contexts,~~ which do not meet the security criterium ~~criterium/criteria~~ when

security protection is required for an access point connection (PDP context~~), i.e. a security protection condition is met~~.

28. (Currently Amended) A packet data support node according to claim 24, ~~characterized in~~ wherein that a security condition is met when a request is received relating to activation of a PDP context to a security indicated APN.

29. (Currently Amended) A ~~pcket~~ packet data support node according to claim 24, ~~characterized in~~ wherein that a security condition is met when a PDP context to a security marked APN is activated.

30. (Currently Amended) A packet data support node according to claim 29, ~~characterized in~~ wherein that the packet data support node comprises means for re-activation of deactivated PDP contexts, and in that said means are end user controlled.

31. (Currently Amended) A node in a mobile communication system supporting communication of packet data and wherein said communication system including a packet data support node, comprising:

security indicating means for providing access points with a security indication to allow for secure remote access connections to corporate networks, ~~characterized in that~~ wherein the security indicating means further provides ~~comprises are associated with~~ a distribution functionality such that a security indication can be distributed to a packet data support node ~~(SGSN; CGSN)~~, that said security indicating means support provisioning of an access point with a security criterium indication indicating which~~, if any,~~ access point connections are allowed simultaneously over the access point.

32. (Currently Amended) A node according to claim 31, ~~characterized in~~ wherein that the security indication is provided to an Access Point Name of the access point.

33. (Currently Amended) A node according to claim 32, ~~characterized in~~ wherein that an access point connection comprises a PDP context and in that the security criterium indication comprises an indication of which criteria~~, if any,~~ that have to be fulfilled by concurrent~~/conflicting~~ access point connections in order to be allowed~~/prohibited~~ when an access point is security indicated.

34. (Currently Amended) A node according to ~~any one of claims 31-33~~ claim 31, ~~characterized in~~ wherein that it comprises a Gateway GPRS Support Node (GGSN).

35. (Currently Amended) A node according to ~~any one of claims 31-33~~ claim 31, ~~characterized in~~ wherein that it comprises a Domain Name Server (DNS).

36. (Currently Amended) A node according to claim 35, ~~characterized in~~ wherein that the Domain Name Server comprises an extended functionality for storing IP addresses and security indications, the DNS server comprising dedicated or specific records for or comprising security indications.

37. (Currently Amended) A node according to ~~any one of claims 31-33~~ claim 31, ~~characterized in~~ wherein that it comprises a Home Location Register (HLR).

38. (Currently Amended) A method for enhancing security of end user station access to Internet ~~and intranet(s), e. g. corporate access, characterized in that it comprises~~ and intranet, comprising the steps of:

establishing if ~~a~~ an access point needs to be secure ;

if yes,

providing the access point ~~(identifier)~~ with a security indication with one or more criteria in a network node,

distributing the security indication to a packet data support node,

enforcing the security indication by at least preventing all traffic on all access point connections conflicting a first security indicated access point connection ~~to/through~~ through the security indicated access point and not

fulfilling the security ~~criterium/criteria~~ criteria at least until the last packet of the security indicated access point connection has been sent.

39. (Currently Amended) A method according to claim 38, ~~characterized in~~ wherein that it comprises the step of:

providing the security indication in a gateway packet data node~~, e.g. a GGSN,~~ in a home location register (HLR) or in a Domain Name Server (DNS).

40. (Currently Amended) A method according to claim 38 ~~or 39~~, ~~characterized in~~ wherein that the step of providing a security indication comprises,

providing an Access Point Name (APN) with the security indication.

41. (Currently Amended) A method according to claim 40, ~~characterized in~~ wherein that the access point connections comprise PDP contexts.

42. (Currently Amended) A method according to claim 41, ~~characterized in~~ wherein that the enforcing step comprises:

dropping all ~~traffical~~ traffic packets of all other PDP contexts than a first incoming security requiring PDP context which do not meet the security ~~criterium/criteria~~ criteria.

43. (Currently Amended) A method according to claim 41, ~~characterized in~~ wherein that the enforcing step comprises:

deactivating all other conflicting PDP contexts than a first security requiring PDP context, which do not fulfill the security criteria ~~criterium/criteria~~.